UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,684	01/04/2007	Yuichi Futa	2006_0401A	3546

52349 7590 03/03/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Response to Arguments

Applicant has amended the independent claim to try to distinguish the claimed invention from the prior art. By limiting the scope, further search and consideration is necessary to determine if having the first encryption key being distinct from the first hash key, is known in the art.

In response to Applicant's arguments that the combination of Diffie and Devadas fail to teach the previously presented limitation, Examiner respectfully disagrees. Specifically in regards Devadas, Examiners find that Devadas teaches a first hash key, calculating using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, and wherein the second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matched the calculated second hash value (0193-0194). Diffie uses the two parts of the keys to form a session key whereby data is encrypted. Devadas uses an encryption key or session key as a MAC key [hash key]. The MAC then hashes message with the encryption key to produce an encrypted message with a hash value. Devadas uses this

known method of message authentication code to further secure the data packet during transmission. This MAC prevents tampering of the packets. Examiner finds the combination of Devadas' teaching of the user of a MAC and hash key provides assurance against tampering to the method of Diffie.

/M. R. V./

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431